

Attorney Docket No. 990301

**IN THE CLAIMS**

Please amend the claims as follows:

1. (Currently Amended) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device ~~through an interface~~;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

loading updating said resident software with said available software ~~into said storage device~~ if said resident software has not been authenticated; and

setting an authentication flag if said resident software is not authenticated but said available software is authenticated.

2. (Currently Amended) A method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device ~~through an interface~~;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

loading updating said resident software with said available software if one of the following three conditions is met:

(1) said resident software is not authenticated and said available software is are authenticated,

(2) said resident software and said available software are not authenticated,

(3) said resident software is not authenticated but said available software is authenticated.

3. (Previously Presented) The method of claim 2 wherein said determining whether or not said resident software is authenticated comprises of:

Attorney Docket No. 990301

determining whether or not an authentication flag has been set;  
wherein said resident software is determined to be authenticated if an authentication flag has been set; otherwise  
said resident software is determined to be unauthenticated.

4. (Currently Amended) The method of claim 3 wherein said authentication flag is set when said authenticated software is loaded onto said computing device if said resident software is not authenticated but said available software is authenticated.

5. (Previously Presented) The method of claim 4 wherein said authentication flag is set by a service technician.

6. (Previously Presented) The method of claim 2 wherein said determining whether or not said resident software is authenticated comprises of performing a direct authentication procedure on said resident software.

7. (Previously Presented) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

8. (Previously Presented) The method of claim 6 wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

9. (Currently Amended) An apparatus for performing configuration management for a computing device, comprising:

an interface for providing available software to be loaded into said computing device to update a resident software within said computing device;

a storage device for storing said resident software and a set of executable computer instructions for determining whether or not said available software and said resident software are authenticated;

a processor for executing said set of executable computer instructions and for: loading updating said resident software with said available software ~~into said computing device~~ if said resident software is not authenticated; and

setting an authentication flag if said resident software is not authenticated but said available software is authenticated.

10. (Currently Amended) An apparatus for performing configuration

management for a computing device, comprising:

an interface for providing available software to be loaded into said computing device to update a resident software within said computing device;

a storage device for storing said resident software and a set of executable computer instructions for determining whether or not said available software and said resident software are authenticated;

a processor for executing said set of executable computer instructions and for:

rejecting said available software if said resident software has been authenticated and said available software is not authenticated; and

~~loading~~ updating said resident software with said available software if one of the following three conditions is met:

(1) ~~said resident software is authenticated~~ and said available software ~~is~~ are authenticated,

(2) said resident software and said available software are not authenticated,

(3) said resident software is not authenticated but said available software is authenticated.

11. (Previously Presented) The apparatus of claim 10 wherein:

said storage device is further for storing an authentication flag for indicating the authentication status of said computing device; and

said processor is further for determining whether or not said resident software is authenticated based on said authentication flag.

12. (Currently Amended) The apparatus of claim 11 wherein said authentication

flag is set when said authenticated software is loaded onto said computing device if said resident software is not authenticated but said available software is authenticated.

13. (Currently Amended) The apparatus of claim 12[[1]] wherein said

authentication flag is set by a service technician.

14. (Previously Presented) The apparatus of claim 10 wherein said processor is

further for performing a direct authentication procedure on said resident software to determine whether or not said resident software is authenticated.

15. (Previously Presented) The apparatus of claim 14 wherein said performing a direct authentication procedure comprises performing a cyclic redundancy check.

16. (Previously Presented) The apparatus of claim 14 wherein said performing a direct authentication procedure comprises performing a secure hashing algorithm.

17. (Currently Amended) An apparatus for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to update a resident software within said computing device ~~through an interface~~;

means for determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for ~~loading~~ updating said resident software with said available software ~~into said storage device~~ if said resident software has not been authenticated; and

means for setting an authentication flag if said resident software is not authenticated but said available software is authenticated.

18. (Currently Amended) An apparatus for implementing a method for configuration management for a computing device, comprising:

means for providing available software to be loaded into said computing device to update a resident software within said computing device through an interface;

means for determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

means for determining whether or not said available software is authenticated;

means for rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

means for ~~loading~~ updating said resident software with said available software if one of the following three conditions is met:

(1) said resident software is not authenticated and said available software ~~is~~ are authenticated,

(2) said resident software and said available software are not authenticated,

(3) said resident software is not authenticated but said available software is authenticated.

19. (Currently Amended) A computer-readable medium embodying codes for implementing a method for configuration management for a computing device, the method comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device ~~through an interface~~;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

~~loading~~ updating said resident software with said available software ~~into said storage device~~ if said resident software has not been authenticated; and

setting an authentication flag if said resident software is not authenticated but said available software is authenticated.

20. (Currently Amended) A computer-readable medium embodying codes for implementing a method for configuration management for a computing device, comprising:

providing available software to be loaded into said computing device to update a resident software within said computing device ~~through an interface~~;

determining whether or not said resident software stored in a storage device associated with said computing device is authenticated;

determining whether or not said available software is authenticated;

rejecting said available software if said resident software is authenticated and said available software is not authenticated; and

~~loading~~ updating said resident software with said available software if one of the following three conditions is met:

(1) said resident software is ~~authenticated~~ and said available software ~~is~~ are authenticated,

(2) said resident software and said available software are not authenticated,

(3) said resident software is not authenticated but said available software is authenticated.